National Infrastructure Protection Center
CyberNotes

Issue #2000-10 ***May 22, 2000***

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 5 and May 18, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
@Stake Inc.[1] Windows, Unix	AntiSniff 1.0.1, Researchers Version 1.0	A buffer overflow vulnerability exists which can be exploited by a remote malicious user to execute arbitrary code on the system.	New versions available at: Version 1.1 http://www.l0pht.com/antisniff/dist/anti_sniff_researchv1-1.tar.gz Version 1.02 http://www.l0pht.com/antisniff/dist/as-102.zip	AntiSniff DNS Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Alexander Siegel[2] Unix	Golddig 2.0	A vulnerability exists in the SUID-level creator application, which could let a local malicious user overwrite any file on the system.	FreeBSD patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-3-stable/games/golddig-2.0.tgz Platforms other than FreeBSD should remove the setuid bit.	Golddig Game Arbitrary File Overwrite	**High**	Bug discussed in newsgroups and websites.

[1] L0pht Advisory, May 18, 2000.
[2] FreeBSD Security Advisory, FreeBSD-SA-00:16, May 9, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Allaire[3]	ClusterCATS ColdFusion	Under certain conditions ClusterCATS appends stale query string arguments to a URL. Some sites using ColdFusion may place usernames and passwords in the stale information.	Patch available at: ftp://ftp.allaire.com/outgoing/clustercats/teserver.dll Versions of ColdFusion prior to 4.5.1 must upgrade to 4.5.1 before applying the patch.	ClusterCATS URL Redirect	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Allaire[4]	Cold Fusion Server 4.5.x, Professional & Enterprise	A remote Denial of Service vulnerability exists when a cached file, which is no longer stored in memory and contains a CFCACHE tag, is requested.	Allaire released patches on January 4, 2000 regarding potential information leakage by the CFCACHE tag, which will also clear up this vulnerability. Patch available at: http://download.allaire.com/AllaireSecurityBulletin(ASB00-03)New4.0xCfcache.zip Create a backup of the existing CFCACHE.CFM file and then copy the new CFCACHE.CFM file to the \CFUSION\BIN\CFTags\ directory.	ColdFusion Cached File Request Remote Denial of Service	**Low/ High (High if DDoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
America Online[5] Windows 95/98/NT 4.0, CE 3.0; MacOS 9.0	Instant Messenger (AIM) 4.0	A vulnerability exists which discloses the full local path of a file transmitted through AIM to the remote recipient. This information could be used in order to discover crucial information about the target (such as the operating system platform) and may assist in a future attack.	No workaround or patch available at time of publishing.	AIM Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Axent[6] Windows NT 4.0	NetProwler 3.0	A Denial of Service vulnerability exists if two fragmented IP packets are sent to the IP of a machine that is currently being monitored.	No workaround or patch available at time of publishing.	NetProwler Fragmented IP Packets DoS	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Cayman[7]	220-H DSL Router 1.0, GatorSurf 5.5Build R0, 5.3Build R2, 5.3Build R1	A Denial of Service vulnerability exists when a large username or password string is sent to the Cayman HTTP admin interface.	No workaround or patch available at time of publishing.	DSL Router Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[3] Allaire Security Bulletin, ASB00-12, May 8, 2000.
[4] Securiteam, May 13, 2000.
[5] Securiteam, May 15, 2000.
[6] RFP2K05, May 18, 2000.
[7] Bugtraq, May 5, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cisco[8] ***Patch now available***[9]	**IOS 11.0, 11.2x, 11.3x, 12.0x**	**A Denial of Service vulnerability exists if remote administration via HTML interface is enabled.**	**No workaround or patch available at time of publishing.** **Temporary workaround:** **(Securiteam)** **Turn off management via HTTP with the following configuration:** ***no IP http server*** ***For software versions and fixes see information table at:*** http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml#Software	**Cisco IOS HTTP Denial of Service**	**Low/ High (High if DDoS best-practices not in place)**	**Bug discussed in newsgroups and websites. Exploit has been published.**
George Burgyan[10]	CGI Counter 4.0.2, 4.0.7	An unchecked user input vulnerability exists which could allow the execution of arbitrary commands by a malicious user.	No workaround or patch available at time of publishing.	CGI Counter Input Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Intel Corporation[11]	NetStructure 7180.0, 7110.0	A vulnerability exists in the default configuration, which could allow remote root access. Additionally, web based management authentication is done in cleartext, which makes the communications vulnerable to local network sniffing.	Patch for the remote backdoor vulnerability is available at: (CD8000) Security Patch http://216.188.41.136/	NetStructure Undocumented Password and Remote Backdoor	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
KDE[12] Unix	KDE 1.1, 1.1.1, 1.2, 2.0 BETA	A vulnerability exists which allows the SHELL variable to be altered to execute something other than the shell. This lets a local malicious user gain UID disk, which can then be used to gain root.	No workaround or patch available at time of publishing.	KDE Kscd SHELL Environmental Variable	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Matt Wright[13] Unix	FormMail 1.6	A vulnerability exists in the FromMail script, which could allow several environment variables to be viewed by a remote malicious user, who can gain useful information about the site. This could make further attacks more feasible.	No workaround or patch available at time of publishing.	FormMail Environmental Variables Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[8] Securiteam, Mar 2, 2000.
[9] Securiteam, May 17, 2000.
[10] Securiteam, May 17, 2000.
[11] L0pht Research Labs Security Advisory, May 8, 2000.
[12] Bugtraq, May 17, 2000.
[13] Perfecto's Black Watch Labs Advisory, BWL 00-06, May 10, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Matthew Redman[14]	Allmanage 2.6	Multiple vulnerabilities exist in the Web Site Administration software package. The admin password is stored in plaintext, which a remote malicious user could easily retrieve. If the upload portion of the CGI is enabled, it is possible for a remote malicious user to browse, delete and upload files because of a vulnerability in the authentication mechanism.	No workaround or patch available at time of publishing.	Allmanage Administrator Password Retrieval	Medium	Bug discussed in newsgroups and websites.
Microsoft[15] Windows 95/98 NT 4.0/2000	Access 2000, Excel 2000, FrontPage 2000, Office 2000, Outlook 2000, PowerPoint 2000, Photodraw 2000.1, Project 2000, Works 2000	A security vulnerability exists in the UA Control, which is incorrectly marked as "safe for scripting." Because of the incorrect marking, a malicious web site operator could use the control to take inappropriate actions on the machine of a visiting user.	Patch available at: Microsoft Office 2000: http://download.microsoft.com/download/office2000pro/Uactlsec/2000/WIN98/EN-US/Uactlsec.exe	Office 2000 UA Control	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Microsoft[16] Windows 98/98/NT 4.0	Outlook 98, Outlook Express 4.x	A remotely exploitable buffer overflow vulnerability exists when a long file name with a graphic (.gif, .jpg) extension is received which could allow the execution of arbitrary code.	Patches available at: Microsoft Outlook 98: http://officeupdate.microsoft.com/downloadDetails/outptch2.htm Microsoft Outlook Express: http://www.microsoft.com/windows/ie/security/oelong.asp	Outlook Long Filename	**High**	Bug discussed in newsgroups and websites.
Microsoft[17] Windows NT 2000	Windows 2000 Server & Professional	A vulnerability exists in the default configuration of SYSKEY, which could permit a compromise of the Encrypting File System (EFS). A malicious user could retrieve this key and decrypt the file system.	No workaround or patch available at time of publishing.	Windows 2000 Default SYSKEY Configuration	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[14] Bugtraq, May 16, 2000.
[15] Microsoft Security Bulletin, MS00-034, May 12, 2000.
[16] Securiteam, May 13, 2000.
[17] Internet Security Systems SAVANT Windows 2000 Advisory No, 00/26, May 10, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft [18] Windows 95/98/NT 4.0/2000	Hotmail	A security vulnerability exists which could allow a malicious user to break into someone's Hotmail account by sending that person an e-mail message with an attached HTML file.	Microsoft has announced that this problem was fixed, and Hotmail is no longer vulnerable to this problem.	Hotmail JavaScript Attachment	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerabilty has appeared in the Press.
Microsoft [19] Windows NT 4.0	Internet Information Server (IIS) 4.0, 5.0	Two security vulnerabilities exist which could be used to slow an affected web server's response or to remotely obtain the source code of certain types of files.	Patch available at: Internet Information Server 4.0: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20905 Internet Information Server 5.0: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20903	Undelimited .HTR Request and File Fragment Reading via .HTR	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft [20] Windows NT 4.0/2000	Internet Information Server (IIS) 4.0, 5.0	A Denial of Service vulnerability exists when a specially crafted URL containing malformed file extensions is sent.	Patch available at: Internet Information Server 4.0: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20906 Internet Information Server 5.0: Http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20904	Malformed Extension Data in URL	**Low/ High (High if DDoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Microsoft [21] Windows NT 4.0	Internet Information Server (IIS) 4.0, 5.0; FrontPage	A vulnerability exists which could expose the physical path of a HTML, HTM, ASP or SHTML when the requested file does not exist.	No workaround or patch available at time of publishing.	IIS shtml.exe Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [22] Windows 95/98/NT 4.0/2000	Active Movie Control 1.0	A vulnerability exists in the Active Movie Control (a multimedia ActiveX control) which could let a malicious user download files of any type specified in the control parameters in an HTML document. This vulnerability could be used in conjunction with other exploits to run arbitrary code on the target machine(s).	No workaround or patch available at time of publishing.	Active Movie Control Filetype	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[18] Securiteam, May 11, 2000.
[19] Microsoft Security Bulletin, MS00-031, May 10, 2000.
[20] Microsoft Security Bulletin, MS00-030, May 12, 2000.
[21] Securiteam, May 16, 2000.
[22] Bugtraq, May 13, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[23] Windows 3.1/95/98/NT 3.51, 4.0, 2000	Internet Explorer 4.0, 5.0, 5.01, 5.5 preview	The DocumentComplete() function in IE does not properly validate origin domains, which could allow a remote malicious web site operator the ability to read, but not change or add, files on the computer of a visiting user.	Patch available at: http://www.microsoft.com/windows/ie/download/critical/patch6.htm	Frame Document Verification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[24] Windows 3.1/95/98/NT 3.51, 4.0, 2000	Internet Explorer 4.0, 5.0, 5.01, 5.5 preview	An unchecked buffer vulnerability exists in the code used to invoke ActiveX components in IE which could allow a malicious web site operator to run code on the computer of a visiting user. The unchecked buffer is only exposed when certain attributes are specified in conjunction with each other.	Patch available at: http://www.microsoft.com/windows/ie/download/critical/patch6.htm	Malformed Component Attribute	Medium	Bug discussed in newsgroups and websites.
Microsoft[25] Windows 95/98/NT 4.0	Internet Explorer 3.x, 4.x, 5.0	By embedding certain escaped characters in the URL, a malicious web site can view the user's cookie entries of another target domain.	Patch available at: http://www.microsoft.com/windows/ie/download/critical/patch6.htm	Internet Explorer Cookie Disclosure	Low	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Microsoft[26] Windows NT 4.0	SQL Server 6.0, 6.5, 7.0	A buffer overflow vulnerability exists in the extended stored procedure, xp_sprintf, which could allow a malicious user to crash the server or to possibly gain admin privileges on the system running SQL Server.	This issue is resolved in the version of Microsoft SQL Server greater than 6.5 SP5.	SQL Server Xp_sprintf buffer	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[27] Unix	John Donoghue Knapster 0.9; Josh Guilfoyle Gnapster 1.3.8	A vulnerability exists which could allow a remote malicious user to view any file on the local system which is accessible to a user running any type of "napster" program.	John Donoghue Knapster 0.9: http://knapster.netpedia.net/#DOWNOAD Josh Guilfoyle Gnapster 1.3.8: http://download.sourceforge.net/gnapster/gnapster-1.3.9.tar.gz FreeBSD: http://www.freebsd.org.ports	Gnapster & Knapster File Access	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[23] Microsoft Security Bulletin, MS00-033, May 17, 2000.
[24] Microsoft Security Bulletin, MS00-033, May 17, 2000.
[25] Microsoft Security Bulletin, MS00-033, May 17, 2000.
[26] ISSalert, May 9, 2000.
[27] FreeBSD Security Advisory, FreeBSD-SA-00:18, May 9, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[28] Windows 95/98, Unix	Gossamer Threads DBMan 2.0.4	A security vulnerability exists when the db.cgi script is opened, which could allow a malicious user to view several environment variables. The parameters displayed include the local document root path, server administrator account name, web server software, platform, etc.	Vendor Patch or workaround: http://www.gossamer-threads.com/scripts/dbman	Gossamer Threads DBMan Information Leakage	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[29]	Cygnus Network Security 4.0.x, KerbNet 5.0.x; MIT Kerberos 4 4.0 patch 10, 5 5.0-1.1.1, 5 5.0-1.0.x	Several buffer overrun vulnerabilities exist which could allow a remote malicious user to gain root access.	Patches are available against krb5-1.0.x., and krb5-1.1.1 MIT Kerberos 5 5.0-1.1.1: http://www.securityfocus.com/data/vulnerabilities/patches/krb5-1.1.1.patch MIT Kerberos 5 5.0-1.0.x: http://www.securityfocus.com/data/vulnerabilities/patches/krb5-1.0.x.patch MIT will release krb5-1.2 shortly, which will remedy these problems in the MIT codebase	Kerberos Compatibility krb_rd_req() Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
NetBSD[30] ***Patch now available[31]***	**NetBSD 1.4.2 SPARC, Alpha; 1.4.1 SPARC, Alpha; 1.4 SPARC, Alpha**	**A Denial of Service vulnerability exists when a packet is remotely sent with an unaligned IP timestamp option.**	**No workaround or patch available at time of publishing.** ***The fix involves changes to two files which are available at:*** ***NetBSD 1.4.1 (and earlier)*** ftp://ftp.NetBsd.ORG/pub/NetBSD/misc/security/patches/20000507-ipopt141 ***NetBSD 1.4.2:*** ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/2000507-ipopt142	**NetBSD Unaligned IP Option Denial of Service**	**Medium/ High** **(High if DDoS best-practices not in place)**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Netopia[32]	R9100 DSL Router 4.6.2, R3100-T Router v4.6	A vulnerability exists in the router, which could allow a malicious user, who already has access to the router, to modify SNMP tables.	Upgrade available at: http://www.netopia.com/equipment/purchase/fmw_update.html	Netopia DSL Router	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape[33]	Navigator & Communicator 4.05-4.07, 4.0, 4.5, 4.5BETA, 4.51, 4.6, 4.61, 4.7, 4.72	A vulnerability exists in the way SSL certificates are validated, which could make it possible for the integrity of an SSL connection to be compromised.	Upgrade available at: http://home.netscape.com/download/	Netscape SSL Certificate Warning Bypass	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[28] Perfecto's Black Watch Labs Advisory, BWL 00-05, May 5, 2000.
[29] ANSIR Advisory, May 19, 2000.
[30] NHC 20000504a.0, May 4, 2000.
[31] Bugtraq, May 7, 2000.
[32] Security Advisory, Netopia R9100 DSL Router, May 8, 2000.
[33] ACROS Security Problem Report, 2000-04-06-1-PUB, May 10, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netwin[34] Windows 9/98/NT 4.0, Unix, MacOS 9.0	DNews 5.3	A unchecked buffer overflow vulnerability exists which could be exploited directly from any browser. This could allow the execution of arbitrary code on the remote target.	Patch available at: ftp://ftp.netwinsite.com/pub/dnews/beta/	Netwin DNews News Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
NetworkICE[35] Windows NT 4.0	ICECap Manager 2.0.23 and previous	Several vulnerabilities exist which could allow a malicious user to log onto the console. The first problem is that the software uses a default login of 'iceman', with no password. The second problem is that the software uses, by default, the Microsoft Jet 3.5 engine to store alerts.	Upgrade available at: http://update.networkice.com/cgi/ic2023a.exe The license key and current version number is required to download the upgrade.	NetworkICE ICECap Manager Default Username and Password	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
NT.Mailserver.com[36] Windows NT 4.0	NTMail 5.0	The server can be configured as a proxy server as well as a web configuration server. A vulnerability exists in the proxy function, which could allow a malicious user to reconfigure their proxy setup to point to NTMail on port 8000, redirecting them to the Internet with no restrictions.	Unofficial workaround: (NTSecurity) The workaround is to disable the WWW configuration service until a patch is released.	NTMail Server 5.x Proxy Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Qualcomm[37]	Eudora Pro, Eudora Light 3.0	A buffer overflow vulnerability exists when the attachment of an e-mail contains a long filename.	No workaround or patch available at time of publishing.	Qualcomm Eudora Pro Long Filename Attachment	Low	Bug discussed in newsgroups and websites.
Seattle Labs[38] Windows NT 4.0	Emurl 2.0	A product design flaw exists which could allow a malicious user the ability to access any mailbox on the system without a password. If identical mailboxes exist on two or more systems, an intruder can use the same URL to access the mailbox on all those systems.	Seattle Labs is aware of the issue and will address it in their next version of Emurl.	Seattle Lab Emurl 2.0 Email Account Access	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[34] Cerberus Information Security Advisory, CISADV000505, May 5, 2000.
[35] RFP2K04, May 16, 2000.
[36] Securiteam, May 15, 2000.
[37] Bugtraq, May 15, 2000.
[38] Bugtraq, May 15, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun Microsystems [39] Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability in the netpr application exists which could allow local malicious users to gain root privileges.	Sun has patches available for this vulnerability. At the present time, they are only available to contract customers.	Solaris Netpr Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Zedz Consultants [40] Unix	Ssh-1.2.27-8i.src.rpm 1.2.27-8i	A vulnerability exists in the RedHat Linux RPM package distributed by Zedz Consulting, which could lead to root access. Due to a flaw in authentication functions, it is possible for a malicious user to log in to any valid account via ssh.	If your ssh installation is vulnerable, you should remove this version and install version 1.2.27-7us.	Zedz Consultants ssh-1.2.27-8i.src.rpm Access Verification	High	Bug discussed in newsgroups and websites. Exploit has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 5 and May 18, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 59 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 18, 2000	Antisniffexpl2.c	Exploit script for the AntiSniff DNS overflow vulnerability.
May 18, 2000	Dnslong.c	Exploit script for the AntiSniff DNS overflow vulnerability.
May 18, 2000	Klogin-bsdi.c	Exploit script for the Kerberos Compatibility krb_rd_req() buffer overflow vulnerability.

[39] Bugtraq, May 12, 2000.
[40] Sword & Shield Enterprise Security, Inc. Security Advisory, May 10, 2000.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 18, 2000	Lo.c	Exploit script for the AntiSniff DNS overflow vulnerability.
May 18, 2000	**RFProw.c**	**Denial of Service exploit for the Axent NetProwler Fragmented IP Packets vulnerability.**
May 17, 2000	Arping-0.2.tar.bz2	An ARP level ping utility that broadcasts a who-has ARP packet on the network and prints answers.
May 17, 2000	Dsniff-2.0.tar.gz	A suite of utilities that are useful for penetration testing.
May 17, 2000	Fdmnt-smash2.c	Local root exploit script for the fdmount vulnerability.
May 17, 2000	Nessus-1.0.0.tar.gz	Full-featured remote security scanner for Linux, BSD, Solaris and some other systems.
May 17, 2000	RFP2K04.txt	Demo exploit script for the RFPickaxe vulnerability.
May 17, 2000	Saint-2.0.2.tar.gz	Security assessment tool based on SATAN.
May 17, 2000	Saint-2.1beta1.tar.gz	Security assessment tool based on SATAN.
May 17, 2000	Syrin15.zip	Win32 tool that "brute forces" the daemon by means of injecting a user specified parameter or command with a value of a user specified number of characters to the daemon.
May 14-16, 2000	011.txt	Technique for exploiting the Matt Kruse Calander vulnerability.
May 14-16, 2000	**7350kscd.tar.gz**	**Exploit script for the KDE kscd vulnerability.**
May 14-16, 2000	CiscoDoS.c	Denial of Service exploit script for the Cisco 760 series router vulnerability.
May 14-16, 2000	Ftpexp.c	Linux exploit script for the STP Server getwd() overflow vulnerability.
May 14-16, 2000	Ismyasp.pl	IIS ASP source code viewer using the ISM.DLL buffer truncation vulnerability.
May 14-16, 2000	**Netprex.c**	**SPARC/i386 buffer overflow root exploit script for the /usr/lib/lp/bin/netpr vulnerability.**
May 14-16, 2000	**Netprx_x86.c**	**SPARC/i386 buffer overflow root exploit script for the /usr/lib/lp/bin/netpr vulnerability.**
May 14-16, 2000	**Netprx-sparc.c**	**SPARC/i386 buffer overflow root exploit script for the /usr/lib/lp/bin/netpr vulnerability.**
May 14-16, 2000	Passfing.tar.gz	Perl script that passively fingerprints operating systems based on signatures.
May 14-16, 2000	Sara-3.0.4.tar.gz	Security analysis tool based on the SATAN model.
May 13, 2000	**Freak88.zip**	**Distributed attack suite, which is a Windows Trojan similar to Wintrin00.**
May 13, 2000	Watcheador.zip	Windows application that allows you to view ASP source code using the Index Server vulnerability in IIS 4 and IIS 5.
May 12, 2000	Datapool3.3.tar.gz	Script that combines 106 Denial of Service attacks into one script.
May 12, 2000	Iidos.zip	Script which exploits the Malformed Extension Data in URL vulnerability.
May 12, 2000	Sendfile.pl	Tool which uses echoes to send files to any web server that has an unchecked open() call in a cgi script.
May 12, 2000	Wpc-0_2b.tar.gz	An application that tries to guess usernames and passwords for password-protected web pages.
May 11, 2000	Bugzilla.txt	Perl remote exploit script for the buffer overflow vulnerability in Bugzilla.
May 11, 2000	Cst1.tgz	A script scanner and portscanner written in Java.
May 11, 2000	Napstir.c	Gnapster and possible other napster Denial of Service exploit script.
May 11, 2000	Nis-spoof.c	Spoofs the response from a NIS server to a client.
May 11, 2000	Nscan666b9.zip	Fast and flexible Windows-based portscanner (up to 200 ports/second), which is designed for scanning large networks and gathering related network/host/whois/traceroute/proxy list/domain zone information.
May 11, 2000	Sara-3.0.3.tar.gz	Security analysis tool based on the SATAN model.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 10, 2000	Iisdos.exe	Script which exploits Microsoft's Undelimited .HTR Request and File Fragment Reading via .HTR vulnerabilities.
May 10, 2000	Netsol.c	Exploit for the (patched) security issue with networksolutions.com(easysteps.pl) which would set up a bindshell if run.
May 10, 2000	Saint-2.0.2.beta3.tar.gz	Security assessment tool based on SATAN.
May 10, 2000	Twwwscan.exe	Windows -based www vulnerability scanner which looks for 162 www/cgi vulnerabilities.
May 9, 2000	Defbomb.pl.	Demonstration of a Perl mailbomber.
May 9, 2000	Ethereal-0.8.8.tar.gz	GTK+-based network protocol analyzer that lets you capture and interactively browses the contents of network frames.
May 9, 2000	gnapster-exp.pl	Exploit script for the napster vulnerability.
May 9, 2000	Heimlich.zip	Proof-of-concept tool for Windows 98 which can be used in regards to the eToken vulnerability.
May 9, 2000	Jport2.tar.gz	Java portscanner which works under Linux.
May 9, 2000	Neon_beta4.c	Host or Iplist CGI scanner which checks for 356 vulnerabilities.
May 9, 2000	Nmap-web-1.4.tar	Web interface to Nmap.
May 9, 2000	**Nmap-2.53.tgz**	**Utility for network exploration, which supports ping scanning, many port scanning techniques, and TCP/IP fingerprinting.**
May 9, 2000	OMNI.sh	Windows 98 exploit script for the OmniHTTPd pro vulnerabilities.
May 9, 2000	Palmpower-1.0.1.tar.gz	Palmpower PilotDis is a disassembler for palm binaries.
May 9, 2000	**Srv_gIrCI_81/zip**	**IRC plugin for BO2K v1.0.**
May 5-8, 2000	Aurora.tgz	Project Aurora is Iamagra's non-blind LAN spoofing project.
May 5-8, 2000	**DrPhil**	**BufferOverflOw Security Team SSH Trojan.**
May 5-8, 2000	NOSp00f.c	Simple module to prevent people from using your box as a launch base for spoofed IP packets.
May 5-8, 2000	OMBRa.c	Linux kernel 2.2.x exploit script.
May 5-8, 2000	Routedsex.c	Denial of Service attack against the routed daemon.
May 5-8, 2000	Spider.tgz	Multi-threaded bad permissions finder.
May 5-8, 2000	SSG-arp.c	AIX local root/usr/sbin/zrp exploit script.
May 5, 2000	ADMDNews.zip	Exploit script for the Netwin DNews News Server buffer overflow vulnerability.
May 5, 2000	ADMNews.cpp	Exploit script for the Netwin DNews News Server buffer overflow vulnerability

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

DDoS/DoS:

- An increasing number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.
- Reports of a combination of tools called "Mstream." The purpose of the tool is to enable intruders to utilize multiple Internet connected systems to launch packet-flooding Denial of Service attacks against one or more target systems.

Probes/Scans:

- An increase in scans to port 109 (pop2 exploit).
- There has been an increase in probes to UDP Port 137 (NetBIOS Name Service).
- An increase in DNS from 211.53.208.178 from Korea, Portugal, Taiwan, and Brazil.
- There has been additional discussion concerning the AMDROCKS BIND exploit.
- An increase in exploiting the rpc.sadmind vulnerability.
- **An increase from Brazil in exploits and scans to port 53 are being used against well-known vulnerabilities: the NXT overflow vulnerability, which creates the directory ADMROCKS after entry; and the BIND vulnerability.**
- There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at ports 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.

Other:

- **The New Love Virus (VBS/NewLove) mutates its appearance in an attempt to avoid detection by anti-virus products.**
- **At time of publication, the "I Love You" virus had 30+ variants.**
- **Continuing compromises of systems running various vulnerable versions of BIND (including machines where the system administrator does not realize a DNS server is running).**
- **An increase in amd exploits.**
- An increase in reports of intruders exploiting unprotected Windows networking shares.
- An increase in the number of sadmind hacks.
- An increase in exploitation of unprotected Windows networking shares.
- Reports indicate registry objects being maliciously altered, including point of contact information for domain names, IP address delegations, and autonomous system numbers.
- Forged email headers are being used to bypass weak registry transaction authentication mechanisms.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will now be included in the table where appropriate. Following this table are write-ups of new viruses and

updated versions discovered in the last two weeks. At times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **203** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **328** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Ranking	Common Name	Type of Code	Trends	Date
1	W32 PrettyPark	File	Slight increase	June 1999
2	W32/SKA (aka Happy 99)	File	Slight increase	March 1999
3	VBS/Kakworm	Script	Increase	December 1999
4	W97M Marker	Macro	Steady	August 1998
5	W97M Ethan.A	Macro	Slight decrease	February 1999
6	W95 CIH	File	Steady	April 1999
7	VBS/Freelink	Script	Steady	July 1999
8	VBS/Loveletter	Script	New to table	May 2000
9	W97M Melissa.A	Macro	Steady	April 1999
10	W97M Class	Macro	New to table	September 1998

W32/SouthPark-A (Aliases: Win32.SouthPark.Worm) (Win 32 E-mail-aware Worm): This is an e-mail-aware worm that uses Microsoft Outlook to spread itself as a message attachment. The subject of the message is "Servus Alter." The message body contains the text "Hier ist das Spiel, das du unbedingt wolltest! :-)." The attached file name is "South Park.exe."

Because the virus uses the German language in its e-mails, it is unlikely to become widespread in non-German speaking countries.

If the attached file is run, the virus uses the Microsoft Outlook address book to forward itself.

The virus copies itself into C:\Winguard.exe and changes the registry so that the file runs on the Windows start-up.

If a floppy disk is present in the floppy drive, the worm transfers system files and worm files to it, making it bootable. When a computer is booted from the floppy, the code in the AUTOEXEC.BAT file copies the worm program file to the Windows start-up directory on the hard drive so that it runs the next time Windows is started.

The worm also creates files called C:\WINDOWSSTART.DLL and C:\WINDOWSSYSTEM.DLL. The WINDOWSSTART.DLL file contains the computer boot count. If the count is equal to 1, the worm creates a file SWAPFILE.VXD and writes to it until the hard drive runs out of space.

The file WINDOWSSYSTEM.DLL contains the initial date of the infection.

W95/Kala.15208 (Windows 95 Executable File Virus): This is a Windows virus that adds 15208 bytes to the length of infected files. The virus contains the text: "never touch the kala-marai!".

WM97/Ethan-BD (Word 97 Macro Virus): This virus has been seen in the wild. It is a macro virus, which contains just one macro. Whenever a document is closed there is a 1 in 3 chance of a File/Properties/Summary box appearing on the screen with the title "Ethan Frome." The virus can mix with other viruses to produce a double infection.

WM97/Iseng-B (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Iseng Word macro virus.

If the Help/About menu is chosen the virus displays a dialog box including the text "Ingat Bung Jaga Perssatuan Dan Kesatuan Bangsa." The virus also displays a message box saying: "Please reinstall your Microsoft Office Program."

WM97/Marker-CZ (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Marker-C Word macro virus.

WM97/Marker-DU (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Marker Word macro virus.

On the first of the month, the virus appends information about the infected user to the end of the macrocode as comments. The virus attempts to transfer the infected user's details to an FTP site.

WM97/Marker-DW (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Marker Word macro virus.

Whenever a document is closed, the virus takes the information in File|Properties|Summary, and FTPs it to the Codebreakers site. It also attaches the sent information to the bottom of the macro as comments.

The virus displays a number of message boxes, which appear to have been included from a user's macro.

WM97/Melissa-AS (Word 97 Macro Virus and E-mail Worm): This is an email-aware Word macro virus. If you open an infected document, it sends a message to the first 100 addresses in your Outlook address books. The message has the following characteristics:

Subject: Duhalde Presidente
Message text: Programa de gobierno 1999 - 2004.

An infected file attachment accompanies the message. When an infected document is opened, if the minute plus 2 is equal to the day of the month plus one, the virus changes the contents of the infected document by inserting spaces.

WM97/Melissa-BE (Word 97 Macro Virus and E-mail Worm): This virus has been reported in the wild and is a variant of the well-known Melissa Word macro virus. The virus sends itself to the first fifty people in each Outlook address book.

The messages have the subject 'Important Message From <username>' (where <username> is taken from the current user information settings) and contain the text 'Here is that document you asked for ... don't show anyone else ;-).' A copy of the infected document from which the virus is launched is attached to each message.

WM97/Pathetic-B (Word 97 Macro Virus): This virus has been reported in the wild. It is a macro virus that exits Word as soon as it is opened on any day during May.

WM97/Replog-A (Word 97 Macro Virus): This virus has been reported in the wild. It is a Word macro virus that attempts to run the file I:\Eudora\Sys\Server.exe. It also appends the text 'Active on' and the date to the file I:\Rep.log.

WM97/Thursday-T (Aliases: Thus) (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of WM97/Thursday.

The virus displays the message "Happy Millennium... From Haccess..." between the 1st and 9th of January.

WM97/Vmpck1-DM (Word 97 Macro Virus): WM97/Vmpck1-DM displays a variety of different message boxes if Word is run for more than five hours or the 'About' box is opened.

It the user tries to read the macro code the virus drops, and attempts to run, Joke/Win-Wobble and displays a message box with the title 'Pesen GUSDOR !'.

The virus attempts to hide itself by intercepting the Tools/Macro function.

VBS/FriendMes-A (Aliases: VBS/FriendMess, VBS.FriendMess.A) (Visual Basic Script Worm):
This is an email-aware worm which arrives in the form of an e-mail with the following characteristics:

Subject line: FRIEND MESSAGE
Message text: A real friend sends this message to you.
Attached file: FRIEND_MESSAGE.TXT.vbs

The virus overwrites the AUTOEXEC.BAT file with code that will delete all the files in the Windows and Windows System directories on the computer's next restart. It also contains the mass-mailing code from VBS/LoveLet.

VBS/NewLove-A (Visual Basic Script Worm):

Aliases: VBS/Loveletter.ed, VBS/Loveletter.Gen, VBS_SPAMMER, VBS.Loveletter.FW.A, NEWLOVE.A, VBS/Spammer.A, VBS.Loveletter.FW, Spammer, and Newlove

This virus has been reported in the wild and is a Visual Basic Script virus that mutates its appearance in an attempt to avoid detection by anti-virus products. It is more destructive than the Love Bug because it indiscriminately over-writes computer files with zero-length files, resulting in an unusable system.

The virus chooses a random filename and attempts to forward a mutated version of itself to everybody in your Microsoft Outlook address book. The name of the file it forwards is determined by randomly choosing one of the filenames in your Windows\Recent folder, appended with ".Vbs" (for instance, EXPENSES.XLS becomes EXPENSES.XLS.Vbs).

The filename attached will have one of the following extensions:

Doc.Vbs
Xls.Vbs
Mdb.Vbs
Bmp.Vbs
Mp3.Vbs
Txt.Vbs
Jpg.Vbs
Gif.Vbs
Mov.Vbs
Url.Vbs
Htm.Vbs

The message has the subject line: "FW: <filename>" where filename is the name of the file it is forwarding, with the extension ".Vbs" removed. If the attached infected file is README.DOC.Vbs, then the subject line will be "FW: README.DOC." Because of this, VBS/NewLove-A does not use the same filename or subject line on different infections. The e-mail message has no message text.

The virus attempts to reduce all files on local and remote drives to zero. This means that Windows may stop working correctly, and that your system will not start up properly upon reboot. This virus will not infect users who have disabled Windows Scripting Host (WSH) on their computers. **Users who are blocking any Visual Basic Script filename (the infected message always arrives with end suffix of ".Vbs" on the filename) also will not be affected.**

XM97/Divi-J (Excel 97 Macro Virus): This is an Excel spreadsheet macro virus, which creates a file called BASE5874.XLS in the Excel template directory, and will infect other spreadsheets as they are opened or closed.

The virus adds a flag, in the form of a variable called IVID plus a hexadecimal number, to each file as it is infected. The virus uses this flag to determine whether the spreadsheet has already been infected.

XM97/Laroux-MV (Excel 97 Macro Virus): This virus has been reported in the wild and is a variant of the XM/Laroux Excel spreadsheet macro virus. The virus contains two macros: auto_open and CHECK_FILES.

When a new spreadsheet worksheet is activated, the virus creates a file in the XLSTART subdirectory called RESULTS.XLS, and copies the viral macros into it. This file is automatically opened every time Excel is started. From then on it infects every workbook used.

XM97/Jini-A (Aliases: Ninja, Jini-A (intended), excel97.intended.jini) (Excel 97 Macro Virus): This virus has been reported in the wild and can replicate under certain conditions.

Upon infecting a workbook the virus may delete all other sheets but the active one.

After the infected worksheet has been open for two minutes, the virus renames all the items in the File menu.

It may display a message box containing following text:

> Hye. You have just got me.
> It's shani a little jini. You may call me a virus in your termenology
> It's a good idea taking backup of you files.
> I am friendly but get wild sometimes!
> It looks like you have caught up by a VIRUS

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Acid Shiver + lmacid	v1.0 + 1.0Mod	CyberNotes-2000-07
AOL Trojan		CyberNotes-2000-01
Asylum	**v0.1**	**Current Issue**
AttackFTP		**Current Issue**
BF Evolution	**v5.3.12**	**Current Issue**
BioNet	v0.84 - 0.92	CyberNotes-2000-09
Bla	1.0-5.02	CyberNotes-2000-06
Bla	v1.0 - 5.03	CyberNotes-2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
DeepThroat	v1.0 - 3.1 + Mod (Foreplay)	CyberNotes-2000-05
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
Drat	v1.0 - 3.0b	CyberNotes-2000-09
FakeFTP	Beta	CyberNotes-2000-02
Girlfriend	v1.3x (including Patch 1 & 2)	CyberNotes-2000-05
Golden Retreiver	**v1.1b**	**Current Issue**
Hack`a`Tack	1.2-2000	CyberNotes-2000-06
Hack'A'tack	1.0-2000	CyberNotes-2000-01
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4	CyberNotes-2000-01
InCommand	v1.0 - 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42	CyberNotes-2000-09
Infector	v1.3	CyberNotes-2000-07
iniKiller	**v1.2 - 3.2 Pro**	**Current Issue**
iniKiller	v1.2 - 3.2	CyberNotes-2000-09
Intruder		CyberNotes-2000-01
Kaos	**v1.1 - 1.3**	**Current Issue**
Khe Sanh	**v2.0**	**Current Issue**
Kuang Original	0.34	CyberNotes-2000-01
Magic Horse		**Current Issue**
Matrix	1.4-2.0	CyberNotes-2000-01
Matrix	v1.0 - 2.0	CyberNotes-2000-09
MoSucker		CyberNotes-2000-06
Naebi	v2.12 - 2.39	CyberNotes-2000-09
NetController	v1.08	CyberNotes-2000-07
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
NetTrojan	1.0	CyberNotes-2000-06
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	1.2-1.3	CyberNotes-2000-06
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65	CyberNotes-2000-09
Setup Trojan (Sshare) +Mod Small Share		CyberNotes-2000-06
ShadowPhyre	v2.12.38 - 2.X	CyberNotes-2000-06
ShitHeap		CyberNotes-2000-09
Softwarst		CyberNotes-2000-05
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02

Trojan	Version	Issue discussed
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
Trinoo		CyberNotes-2000-05
TryIt		CyberNotes-2000-05
wCrat	v1.2b	CyberNotes-2000-05

Asylum v0.1(May 7, 2000): This is a very small Trojan whos features include the ability to upload and download files to the infected system, run software, and restart the computer. Its main use is to install other more featured trojans.

AttackFTP (May 7, 2000): This Trojan opens a public FTP server on your computer, and gives anyone access to upload or download files.

BF Evolution v5.3.12 (May 7, 2000): This Trojan appears to be a Back Orifice clone in its features, including the way it loads on startup.

Golden Retreiver v1.1b (May 7, 2000): This Trojan has a single purpose. It is configured with information on where to obtain a second Trojan. Once you are infected, it attempts to download and install the second trojan to your system, and then deletes itself.

iniKiller v1.2 - 3.2 Pro (April 27, 2000): Basic Trojan with a few destructive commands which can easily destroy data on your system.

Kaos v1.1 - 1.3 (May 7, 2000): This is a basic NetBus clone, with the same features.

Khe Sanh v2.0 (May 7th, 2000): This Trojan is a file manager very similar to the Windows Explorer program. It is however, a Trojan which gives others easy access to an infected computer.

Magic Horse (May 7, 2000): This Trojan is an information and password gatherer, which emails its findings to its creators.

Prayer v1.2 - 1.5 (April 29, 2000): This Trojan is not in English; however, it apparently contains quite a number of features. This Trojan can perform file transfers, run programs, restart the computer, etc. It seems to mirror the standard/common features of NetBus.